

Amendments to the Drawings:

The attached drawing sheet includes a replacement sheet for FIG. 1 that has been amended to indicate that it constitutes prior art.

REMARKS

Claims 1-12, 15 and 16 have been withdrawn from consideration. Claims 13, 14 and 19-21 are currently pending, with claims 13 and 19-21 being the independent claims. The Specification has been amended. The drawings have been amended. Claim 13 has been amended. Claims 19-21 have been added. No new matter has been added. Reconsideration of the application, as amended, is respectfully requested.

The Oath/Declaration has been objected to by the Examiner for purportedly for failing to include the inventor's signature. Regarding this objection, an executed declaration that included the inventor's signature was submitted on February 15, 2002, in response to receipt of a Notice to File Missing Parts (Form PCT/DO/EO/905) February 1, 2002. The enclosed copy of the stamped return receipt postcard indicates that a complete Oath/Declaration was received by the Patent Office on February 15, 2002. In any event, Applicant is re-submitting herewith a copy of the Oath/Declaration which includes the inventor's signature. Withdrawal of the objection is therefore in order.

The drawings have been objected to by the Examiner. Specifically, the Examiner has indicated that Fig. 1 should be amended to state that it constitutes prior art and that the drawings include the following reference character(s) not mentioned in the description: 106 and 204. In response to these objections, Applicant has amended Fig. 1 to indicate that it constitutes prior art, as required by the Examiner. In addition, the specification has been amended to indicate reference numerals 106 and 204. Withdrawal of these objections are in order.

The Specification has been objected to based on certain informalities. In response to these objections, Applicant has amended the Specification in a manner that addresses each objection. Withdrawal of the objection to the Specification is in order.

Claims 13 and 14 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. In response to this rejection, Applicant has amended the claims in a manner that is believed to address the specific rejection. Accordingly, reconsideration and withdrawal of the rejections are respectfully requested.

In the Office Action dated December 9, 2005, independent claim 13, and dependent claim 14 were rejected under 35 U.S.C. §101 as inoperative and, thus lacking utility. Specifically, the Examiner has stated, "The receiver merely receives data and compares values. There is no result

from the comparison or the claimed operations”. In response to this rejection, Applicant has amended independent claim 13 to recite the limitation “determine whether the receive data has changed during transmission over the network”. Support for this amendment may be found, for example, at pg. 6, lines 25-27. No new matter has been added. Withdrawal of the rejection is respectfully requested.

In the Office Action dated December 9, 2005, independent claim 13, and dependent claim 14 were rejected under 35 U.S.C. §102(b) as anticipated by U.S. Patent No. 5,694,471 (“*Chen*”). For the following reasons, it is respectfully submitted that all claims of the present application are patentable over the cited reference.

The invention relates to a receiver for receiving data from a transmitter over a telecommunications network without increasing the size of the data packet. In accordance with the claimed invention recited in amended claim 13, per packet authentication is performed so that a receiver can determine if a packet is valid in a single check (see pg. 3 line 35 thru pg. 4, line 2 of the specification). By utilizing the receiver described in amended claim 13, it is possible to protect data that is transmitted from a transmitting device to a receiving device over a telecommunications system, so that even if a number of intermediate devices have access to the transmitted message as it passes over the system, it is not possible for the intermediate devices to make unauthorised intentional modifications and/or sub-optimal transmission conditions may not cause unintentional corruption of data bits, each without causing the receiving device to notice that the data has changed during transmission.

In accordance with one aspect of the invention the claimed authentication value, e.g. a MAC value, is something that can only be calculated by knowing a shared secret key. The authentic sender and the authorised receiver both know what the shared secret key is, but not unauthorised middlemen. Thus, based on the shared reference value, the sender can compose the proper authentication value for a specific piece of data, and the receiver can check to ensure the authentication value matches the data.

On the other hand, an error check value, i.e. a CRC value, is only used to check that the data bits have not changed their values during transmission. The calculation of a CRC value is well known. As result, it is easy to calculate a CRC value to check whether errors in a data packet have occurred. However, shared secret keys, i.e., authentication values, are not needed to calculate this error check value.

Another key principle associated with the present invention is the nature of an exclusive-OR (XOR) logical operation that can be used to “combine” two values into a single result, for example, $a \text{ XOR } b = c$. Similarly, the XOR operation can be used to “reveal” one of the component values from a calculated result if the other component value is known, for example, $c \text{ XOR } b = a$ and $c \text{ XOR } a = b$. In accordance with the present invention, this characteristic of the XOR operation is utilized to ensure that the combined result “transports” both a MAC value (i.e., the authentication value) and the CRC value (i.e., the error check value) over the telecommunications connection from the sender to the receiver. Here, however, only one data field is needed to transport the MAC value and the CRC value, but yet the receiver, from the viewpoint of checking errors and authenticating messages, will still be permitted to process received data separately.

Chen relates to a system and method for preventing counterfeiting of an identification or transaction card, and for verifying that the user of the card is an authorized user (see Abstract). *Chen* (Abstract, lines 3-5) teaches that a unique, unalterable serial number and an exclusive OR function are used to generate a private key protected digital signature. *Chen* (Abstract, lines 6-8) states, “the digital signature is stored on the card together with a card issuer record which contains sufficient information to authenticate the record”.

The Office Action (pg. 5, paragraph 13) states:

Chen discloses a receiver for receiving data (column 9 lines 42-49) including, means for deriving a first reference value from the received data (issuer data, column 9, lines 50-55), means for calculating an error check value from the received data (another checksum, column 9 lines 64-67), means for deriving an authentication value for the received data (composite, column 9 lines 56-62), means for calculating a second reference value (recovered checksum, column 9 lines 62-64) at least partly based on the authentication value and the first reference value (issuer data), and means for comparing the second reference value with the error check value (column 10 lines 2-11).

Applicant respectfully asserts that *Chen* fails to teach the invention recited in amended independent claim 13. *Chen* is directed to ensuring that a “physical” data carrier, such as a credit card or the like, is the original carrier of the data, as opposed to an unauthorised copy or fake. In the claimed invention, data to be protected travels a long way in a relatively abstract form and can contain whatever payload data users wish to communicate between each other, while on the other hand *Chen* teaches that the data to be protected resides on a fixed medium, in a single

memory device and can only be locally read from the memory in order to perform the necessary security checks.

Chen, on the other hand, fails to teach that the a first reference value, such as an XOR operation, is used pursuant to saving bits in a transmission, i.e., preventing transmission errors. Rather, *Chen* (col. 8, lines 1-8) teaches that an XOR operation only associates a certain digital bit string with a permanent, freely available identifier of the physical data carrier upon which the digital bit string is stored. *Chen* (col. 7, lines 61-64) teaches that the performance of a one-way hashing function, where the hashing function is a MAC value, generates a checksum. *Chen* teaches that the checksum is only a hash of two pieces of digital information, i.e., a condensed representation of the contents thereof. Thus, *Chen* does not teach a checksum in the classical meaning of the word. In fact, within the context of *Chen*, the use of the word checksum is improper, because none of the values calculated in *Chen* serve to enable the detection of transmission errors that occur in a telecommunication system. *Chen* clearly fails to teach “a receiver for receiving data from a transmitter over a telecommunications network, the receiver ... having [at least] means for checking received data ... comprising ... means for deriving a first reference value from the data received over the telecommunications network ... means for calculating an error check value from the data received over the telecommunications network ... and means for deriving an authentication value for the data received over the telecommunications network ... to determine whether received data has changed during transmission,” as recited in amended independent claim 13.

Consequently, independent claim 13 is patentable over *Chen* and thus, reconsideration and withdrawal of the rejection under 35 U.S.C. §102 are in order, and a notice to that effect is earnestly solicited.

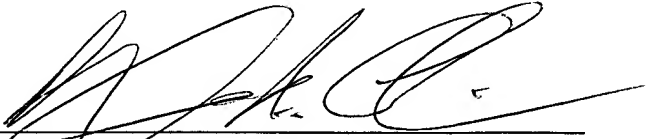
New independent claims 19-21 each recite limitations directed to determining whether a reference value when compared with an error check value indicates that the received data has changed during transmission. *Chen* has nothing to do with this claimed feature. Therefore, new independent claims 19-21 are also patentable over *Chen*.

In view of the patentability of amended independent claim 13, as well new independent claims 19-21, for the reasons set forth above, dependent claim 14 is patentable over the prior art.

Based on the foregoing amendments and remarks, this application is in condition for allowance. Early passage of this case to issue is respectfully requested.

Respectfully submitted,

COHEN, PONTANI, LIEBERMAN & PAVANE

By 

Alphonso A. Collins

Reg. No. 43,559

551 Fifth Avenue, Suite 1210

New York, New York 10176

(212) 687-2770

Dated: April 11, 2006